

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-027296

(43)Date of publication of application : 25.01.2002

(51)Int.Cl.

H04N 5/225

H04N 5/907

H04N 5/765

H04N 7/08

H04N 7/081

// H04N101:00

(21)Application number : 2000-204772

(71)Applicant : FUJI PHOTO FILM CO LTD

(22)Date of filing : 06.07.2000

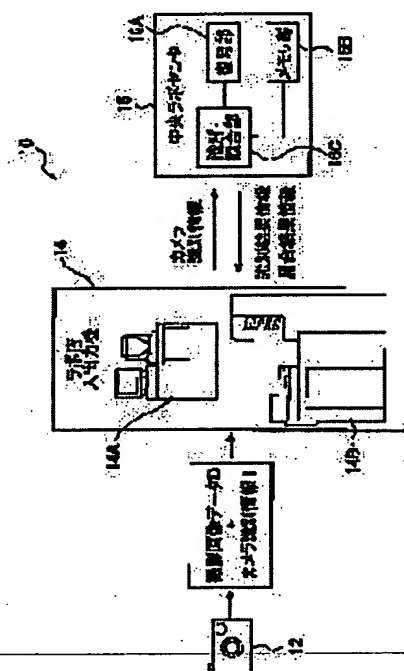
(72)Inventor : KANESHIRO NAOTO

**(54) PROCESSING CONTROL METHOD FOR OUTPUT INFORMATION AND OPERATION CONTROL METHOD FOR UNIT**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide the processing control method of output information, which controls a processing on output information outputted from an information communication unit and an electronic unit, and an operation control method for controlling the operation of the information communication unit and the electronic unit without the trouble of the input of a password and the like.

**SOLUTION:** The unit outputs output information including unit identification information and the presence or absence of the change of unit identification information is judged or collation with unit registration information is performed based on unit identification information. Then, the processing on output information is controlled in accordance with the result of judgment or collation. Consequently, the first unit accesses the second unit by using a communication means when the prescribed operation of the first unit is started or at every prescribed time. Thus, a problem is solved by controlling the operation of the first unit in accordance with operation control instruction information obtained from the second unit.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-27296  
(P2002-27296A)

(43) 公開日 平成14年1月25日 (2002.1.25)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
H 0 4 N	5/225	H 0 4 N 5/225	F 5 C 0 2 2
	5/907	5/907	A 5 C 0 5 2
	5/765	101: 00	B 5 C 0 5 3
	7/08	5/91	L 5 C 0 6 3

審査請求 未請求 請求項の数 8 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願2000-204772(P2000-204772)

(22) 出願日 平成12年7月6日(2000.7.6)

(71) 出願人 000005201

富士写真フイルム株式会社  
神奈川県南足柄市中沼210番地

(72) 発明者 金城 直人

神奈川県足柄上郡開成町宮台798番地 富  
士写真フイルム株式会社内

(74) 代理人 100080159

弁理士 渡辺 望穂

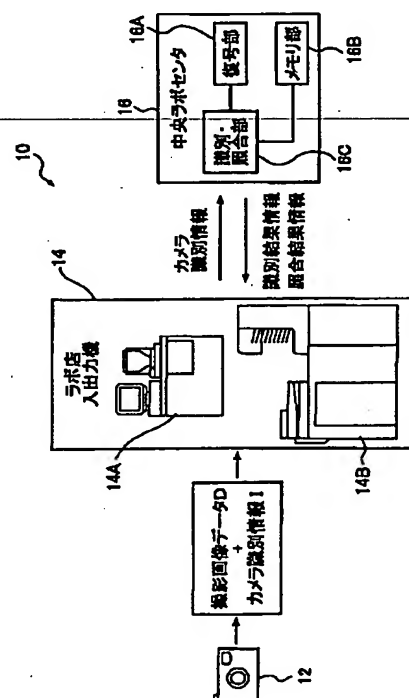
Fターム(参考) 5C022 AA13 AC18 AC69  
5C052 GA02 GA06 GA08 GB09 GC00  
GE06 GE08  
5C053 FA04 FA08 FA27 FA30 GB06  
JA16 JA21 KA05 LA14  
5C063 DA07 DA13

(54) 【発明の名称】 出力情報の処理制御方法および機器の動作制御方法

(57) 【要約】

【課題】パスワード等の入力の手間をかけず、情報通信機器や電子等機器等から出力された出力情報に施す処理を制御する出力情報の処理制御方法、および、情報通信機器や電子等機器等の動作を制御する動作制御方法を提供する。

【解決手段】機器識別情報を含ませた出力情報を機器によって出力し、前記機器識別情報の改変の有無の判断、あるいは、前記機器識別情報に基づく機器登録情報との照合を行い、前記判断あるいは前記照合の結果に応じて、前記出力情報に施す処理を制御することで、また、第1の機器の所定の動作の開始時に、あるいは、一定時間毎に、前記第1の機器から所定の第2の機器に通信手段を用いてアクセスし、前記第2の機器から得られる動作制御指示情報に従って、前記第1の機器の動作を制御することで、前記課題を解決する。



## 【特許請求の範囲】

【請求項1】機器識別情報を含ませた出力情報を機器によって出力し、

前記機器識別情報の改変の有無の判断、あるいは、前記機器識別情報に基づく機器登録情報との照合を行い、前記判断あるいは前記照合の結果に応じて、前記出力情報に施す処理を制御することを特徴とする出力情報の処理制御方法。

【請求項2】前記出力情報は、画像データあるいは撮影画像を有し、

前記機器登録情報に登録されたデータ処理制御指示情報に基づいて、前記画像データあるいは前記撮影画像に施す処理が制御される請求項1に記載の出力情報の処理制御方法。

【請求項3】前記出力情報は、画像データを有し、前記機器識別情報は、前記画像データに付随するヘッダ情報に書き込まれる請求項1または2に記載の出力情報の処理制御方法。

【請求項4】前記出力情報は、画像データを有し、前記機器識別情報は、電子透かし手法によって前記画像データに埋め込まれる請求項1または2に記載の出力情報の処理制御方法。

【請求項5】前記出力情報は、カメラによって記録されたフィルムの撮影画像であり、前記機器識別情報は、磁気情報および光学情報の少なくとも一方として前記フィルムに記録される請求項1または2に記載の出力情報の処理制御方法。

【請求項6】第1の機器の所定の動作の開始時に、あるいは、一定時間毎に、前記第1の機器から所定の第2の機器に通信手段を用いてアクセスし、前記第2の機器から得られる動作制御指示情報に従って、前記第1の機器の動作を制御することを特徴とする機器の動作制御方法。

【請求項7】前記第2の機器と所定の通信を行えない場合、前記第1の機器の前記動作を停止させる請求項6に記載の機器の動作制御方法。

【請求項8】前記第2の機器から動作制御指示情報が得られない場合、あるいは、前記第2の機器と所定の通信を行えない場合、電源投入状況にかかわらず前記第1の機器の所定表示箇所に警告情報を継続表示する請求項6または7に記載の機器の動作制御方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、機器等から出力されるデータ等の出力情報に施す処理を制御する方法、あるいは機器を制御する動作制御方法に関し、特に、デジタルスチルカメラやフィルムを用いて画像を記録するカメラや携帯情報端末（PDA）や携帯電話等の機器から出力された出力情報のデータ処理や上記機器の動作を制御する動作制御方法に関する。

## 【0002】

【従来の技術】近年、情報通信分野の発達に伴い、個人向けの通信機器や電子機器が多数商品化されている。たとえば、携帯電話やPHS等の各種通信機器やこの通信機器を用いて出力データを転送する携帯情報端末（PDA）、静止画像や動画を撮影するデジタルカメラ等のほか、上記携帯情報端末とデジタルカメラ等の撮像手段を組み合わせ、静止画のみならず動画に手書きデータや文書データを合成し、さらに、音声データを加えた出力データを送信する複合化した携帯情報端末も登場している。このような商品は、時代の最先端を行く魅力のある商品として、需要者を強く引きつけるものとなっている。

【0003】しかし、このような需要者を強く引きつける魅力ある情報通信機器や電子等機器等は、一般的に盗難防止機能が付いていないため、盗難にあった商品が売買され、本来使用が許可されていない第3者の手に渡って使用される場合が多い。これは、商品に対する盗難を想定したセキュリティ対策が施されていないために発生するトラブルである。

## 【0004】

【発明が解決しようとする課題】このような状況下、特開平9-284691号公報には、随時パスワードを入力しなければ、画質を劣化させる携帯型映像記録装置が提案されている。すなわち、随時入力の要求されるパスワードを照合し、照合の結果に応じて画質劣化処理を制御するので、正しいパスワードを入力した正規の使用者だけが装置の機能を自由に使用でき、装置の盗難を未然に防止できるとされている。

【0005】しかし、装置がパスワードの入力を要求する度に一々パスワードを入力するのは、使用者にとって煩雑である。また、正規の使用者であってもパスワードを忘れる場合があり、このような場合、装置の機能を自由に使用できなくなる。あるいは、使用者が装置メーカーに使用者設定のパスワードの変更を依頼することもあるが、使用者に余分な負担をかけてしまうといった問題がある。また、第3者に貸し出した情報通信機器や電子等機器等の使用を一定範囲に限定し、機器の動作を制限したい場合もある。さらに、第3者が機器を正常に動作させて出力させた出力データを以降に行なわれる処理に制限を課したい場合もある。

【0006】そこで、本発明は、パスワード等の入力の手間をかけず、情報通信機器や電子等機器等から出力された出力情報に施す処理を制御する出力情報の処理制御方法、あるいは、情報通信機器や電子等機器等の動作を制御する動作制御方法を提供することを目的とする。

## 【0007】

【課題を解決するための手段】上記目的を達成するために、本発明は、機器識別情報を含ませた出力情報を機器によって出力し、前記機器識別情報の改変の有無の判断、あるいは、前記機器識別情報に基づく機器登録情報

10

20

30

40

50

との照合を行い、前記判断あるいは前記照合の結果に応じて、前記出力情報に施す処理を制御することを特徴とする出力情報の処理制御方法を提供する。

【0008】ここで、前記出力情報は、画像データあるいは撮影画像を有し、前記機器登録情報に登録されたデータ処理制御指示情報に基づいて、前記画像データあるいは前記撮影画像に施す処理が制御されるのが好ましい。また、前記出力情報は、画像データを有し、前記機器識別情報は、前記画像データに付随するヘッダ情報に書き込まれるのがよく、あるいは、前記出力情報は、画像データを有し、前記機器識別情報は、電子透かし手法によって前記画像データに埋め込まれるのがよく、あるいは、前記出力情報は、カメラによって記録されたフィルムの撮影画像であり、前記機器識別情報は、磁気情報および光学情報の少なくとも一方として前記フィルムに記録されるのがよい。

【0009】また、本発明は、第1の機器の所定の動作の開始時に、あるいは、一定時間毎に、前記第1の機器から所定の第2の機器に通信手段を用いてアクセスし、前記第2の機器から得られる動作制御指示情報に従って、前記第1の機器の動作を制御することを特徴とする機器の動作制御方法を提供するものである。

【0010】ここで、前記第2の機器と所定の通信を行えない場合、前記第1の機器の前記動作を停止させるのが好ましく、また、前記第2の機器から動作制御指示情報が得られない場合、あるいは、前記第2の機器と所定の通信を行えない場合、電源投入状況にかかわらず前記第1の機器の所定表示箇所に警告情報を継続表示するのが好ましい。

【0011】

【発明の実施の形態】以下、本発明の出力情報の処理制御方法および機器の動作制御方法について、添付の図面に示される好適実施例を基に詳細に説明する。

【0012】まず、本発明の出力情報の処理制御方法の一例として、通信機器や電子機器等の機器から出力された出力データに施される処理の制御の一例を説明する。図1には、カメラで撮影された出力画像データに出力処理を施すプリント画像の作成を制御する、出力データの処理制御システム10が示されている。出力データの処理制御システム10は、画像を撮影するカメラ12と、プリント画像の出力サービスを提供する複数の業者に設けられる入出力機（図1では複数の入出力機の1つを示す）14と、入出力機14と通信接続される中央ラボセンタのコンピュータ16とを備える。

【0013】カメラ12は、CCD撮像素子等を用いて撮影画像の画像データを出力データとして出力する電子機器、すなわちデジタルスチルカメラである。カメラ12は、撮影された撮影画像を撮影画像データDとしてスマートメディア、PCカードやコンパクトフラッシュ（登録商標）カードやFD、Zip™やMO等の各種記

録メディアに記録する。さらに、カメラ12は、撮影時、撮影画像データDのヘッダ情報に、暗号化したカメラ識別情報Iを付随して付加し、撮影画像データDとともに、カメラ12の出力情報として、上記各種記録メディアに記録する。このカメラ識別情報Iは、固有の規則性を持つデータ構成として作成されてカメラ一台ずつに割り当てられ、カメラ一台一台を識別することのできる機器識別情報、例えばID番号（識別番号）等であって、セキュリティを向上のために、予め定められた暗号化方法によって暗号化されている。この暗号化されたカメラ識別情報Iは、復号化されることで、ID番号（識別番号）等を得ることができ、カメラ12を識別することができる。このような固有の規則性を持つデータ構成としたカメラ識別情報Iの暗号化により、カメラ識別情報Iの改変や偽造を困難なものとしている。また、このようなカメラ12のカメラ識別情報Iを正規の使用者は知っており、カメラ12が盗難された場合、中央ラボセンタにカメラ識別情報Iを持つカメラ12が盗難された旨が届け出され、ラボ中央センタのコンピュータ16のメモリ部16Bにカメラ識別情報毎に設けられるカメラ登録情報に、カメラ識別情報Iを持つカメラ12が盗難されたことを示す盗難情報が記録される。また、正規の使用者の届け出によって、カメラ識別情報Iを持つカメラ12で撮影された撮影画像データDの処理を制限するデータ処理制御指示情報が記録される。

【0014】上記例のカメラ識別情報Iは、撮影画像データDのヘッダ情報に付加するものであるが、カメラ識別情報Iを電子透かし手法により撮影画像データの中に付随して埋め込むものであってもよい。電子透かし手法とは、画像を傷付けない範囲で直接撮影画像データDにデジタル的に別の情報を書き込む手法であり、例えば、東芝レビューV o l . 54、No. 7（1999）の12～15ページに記載されているように、スペクトル拡散法に基づいてカメラ識別情報Iを撮影画像データDの中に埋め込むことができ、逆拡散により、カメラ識別情報Iを撮影画像データDの中から検出し抽出することができる。このような撮影画像の画像データDおよびこれに付随したカメラ識別情報Iは、記録メディアによって、あるいは通信回線によって、カメラ12の出力情報として、画像の出力サービスを行なう業者に提供される。

【0015】また、カメラ12は、撮影画像を画像データとして出力するデジタルスチルカメラであるが、フィルムに画像を記録するカメラ、例えば、新写真システム（APS（Advanced Photo System））対応のカメラや135mmサイズのフィルムに対応する通常のカメラであってもよい。この場合、カメラによってフィルムに撮影された撮影画像が出力情報として、画像の出力サービスを行なう業者に提供される。撮影されたフィルムがAPS対応カメラの場合、暗号化したカメラ識別情報IをA

PS用フィルムの画像コマに付随して設けられる磁気記録層に磁気情報として記録され、この磁気情報が、撮影画像とともにカメラの出力情報として出力サービスを行なう業者に提供されるとよい。また、135mmサイズのフィルムに対応する通常のカメラの場合あるいはAPS対応カメラの場合、フィルムの一部分にバーコード表記等によって表され、暗号化されたカメラ識別情報Iが光学情報として光学的に焼き込まれ、この光学情報が撮影画像とともにカメラの出力情報として出力サービスを行なう業者に提供されるとよい。

【0016】入出力機14は、画像の出力サービスを提供する業者に設けられる入出力装置であり、フィルムに記録された画像を読み取り画像データを得るスキャナや、スマートメディア、PCカードやコンパクトフラッシュカードやFD、Zip<sup>TM</sup>やMO等の各種記録メディアに記録された撮影画像データDやカメラ識別情報Iを読み込み、また、場合によっては書き込むことのできる読込書込装置等や、撮影被写体のエッジを強調したり、ぼかししたりするシャープネス補正処理や、ダイナミックレンジの圧縮・伸張処理等の付加価値の高い所望の画像処理等を画像データに施して処理画像データを得るイメージプロセッサ等を備える入力機14Aと、処理画像データに基づいて感光材料を露光するレーザプリンタおよび、露光されて感光材料に記録された潜像を顕像化するプロセッサ等を備えたプリント画像を出力する出力機14Bを有する。なお、撮影画像データDの処理には、プリント画像のプリント出力処理のみならず、付加価値の高い所望の画像処理や、所定の画像との合成処理や、モニタ表示による再生処理や記録メディアに書き込む記録処理も含まれる。

【0017】入力機14Aは、中央ラボセンタのコンピュータ16と送受信可能となるように通信回線で接続を行なうモデムやTA（ターミナルアダプタ）やルータ等の通信回線装置を有する。入力機14Aは、記録メディアに記録された撮影画像データDを取得する際、撮影画像データDに付随してヘッダ情報に付加して記録されたカメラ識別情報Iをヘッダ情報の中の該当する部分から取り出して取得する。取得したカメラ識別情報Iは、直ちに通信回線装置を通して、中央ラボセンタのコンピュータ16に送信されるように構成される。また、入力機14Aは、後述するように、通信回線装置を介して中央ラボセンタのコンピュータ16から送信される情報を受信する。例えば、カメラ識別情報の改変の有無に関する識別結果情報や、機器登録情報と照合を行った結果として得られる盗難情報Aやデータ処理内容に制限を課するデータ処理制御指示情報B等の照合結果情報を受信する。

【0018】入力機14Aは、受信した識別結果情報や盗難情報Aやデータ処理制御指示情報Bに応じて、取得された撮影画像データDに施す画像処理を停止し、従っ

て、処理画像の画像データを記録メディアに書き込む記録処理や、出力機14Bで行なうプリント出力処理を停止し、あるいは、撮影画像データDに施す画像処理等の処理を制御する。撮影画像データDに予め定められている電子透かし手法を用いてカメラ識別情報Iが埋め込まれる場合、入力機14Aは、撮影画像データDからカメラ識別情報Iを検出し抽出する電子透かし情報抽出部を設け、カメラ識別情報Iを検出し抽出するとよい。撮影画像が、フィルムに記録された画像である場合、フィルムをスキャナで読み込む際にフィルムの磁気記録層に記録された磁気情報が、磁気読み取り装置によって読み取られ、暗号化されたカメラ識別情報Iが取得され、あるいは、フィルムの一部分に光学的に暗号化しバーコード表記等で焼き込まれたカメラ識別情報Iが撮影画像をスキャナで読み取られる際、一緒に読み取られ、バーコード表記から、暗号化されたカメラ識別情報Iを取得するとよい。

【0019】中央ラボセンタのコンピュータ16は、複数のラボ店と通信回線装置を通して通信回線で接続され、常時ラボ店の入出力機14の稼働状況やエラー履歴の確認や遠隔診断を行ない、必要に応じて情報を提供する管理制御機能を備えたコンピュータである。コンピュータ16は、さらに、ラボ店の入出力機14から送られてくる暗号化されたカメラ識別情報Iを復号化し、ID番号等のカメラ識別情報Iを取得する復号部16Aと、正規の使用者から届けられた機器登録情報、例えば、盗難情報やデータ処理制御指示情報が蓄積記録されたメモリ部16Bと、カメラ識別情報Iが改変されたか否か識別し、あるいは、復号化されたカメラ識別情報Iから機器登録情報の内容を照合する識別・照合部16Cを備える。

【0020】図2には、メモリ部16Bに記録されている機器登録情報の一例であるカメラ登録情報が示されている。カメラ登録情報は、正式なカメラの使用者によって届け出されたカメラ識別情報I<sub>1</sub>、I<sub>2</sub>、I<sub>3</sub>、...によって区分けされ、届け出内容が階層的に記録されている。例えばカメラ識別情報I<sub>1</sub>の第1階層にはカメラが盗難された旨の盗難情報Aが記録されており、カメラ識別情報I<sub>1</sub>の第1階層にはデータ処理制御指示情報Bが記録され、さらに下の第2階層には、データ処理の制御内容を指示する情報が記録されている。図中では、撮影画像データDのヘッダ情報やフィルムの磁気情報に記録されている撮影日付情報を利用したプリント出力処理の制御内容であって、○月×日以前に撮影された撮影画像データDはプリント出力処理されないといった制御内容である。この他に、プリント出力画像の枚数やプリント出力画像のサイズに制限を加えたり、特殊な画像処理、例えばテンプレート画像との合成処理を禁止する制御内容が挙げられる。

【0021】識別・照合部16Cは、カメラ識別情報I

が固有の規則性を持つデータ構成となっているか識別し、規則性が破壊されていると識別された場合、カメラ識別情報Iに不正な改ざんがあったと判断して、その旨の識別結果情報を作成し、不正な改ざんがない場合、メモリ部16Bに記録されているカメラ登録情報を検索して照合し、カメラ識別情報Iが登録されている場合、記録されている情報、例えば盗難情報Aやデータ処理制御指示情報B等の照合結果を呼び出す部分である。このようにカメラ識別情報の改変の有無に関する判断結果情報や、機器登録情報の照合結果情報がラボ店の入出力機14に送信される。カメラ識別情報Iが改変、偽造されたか否かは、正規のカメラ識別情報Iが固有の規則性を持つデータ構成として作成されていることから、この固有の規則性が破壊されているか否かを識別することにより容易に判断することができる。

【0022】このような出力データの処理制御システム10では、ラボ店の入力出力機14において、カメラ12で撮影された撮影画像データDと、暗号化されたカメラ識別情報Iが、スマートメディアやPCカード等の各種記録メディアから読込書込装置を介して読み取られて取得される。暗号化されたカメラ識別情報Iの取得方法は、カメラ識別情報Iが撮影画像データDのヘッダ情報として記録された場合、カメラ識別情報Iが電子透かし手法により撮影画像データDに埋め込まれた場合、APS用フィルムの磁気記録層に磁気情報として記録された場合、あるいは、フィルムの一部分に光学的に焼き込まれた場合等種々の場合があるが、上述したように各場合にに応じた方法で暗号化されたカメラ識別情報Iが取得される。

【0023】取得されたカメラ識別情報Iは、通信回線装置を介して中央ラボセンタのコンピュータ16に送られる。ここで、まず、カメラ識別情報Iの復号化処理が復号部16Aで行なわれ、復号化された、IDカメラ番号等のカメラ識別情報Iが得られ、識別・照合部16Cに送られる。識別・照合部16Cでは、まず、カメラ識別情報Iが固有の規則性を持つデータ構成となっているか識別し、規則性が破壊されていると識別された場合、カメラ識別情報Iに不正な改ざんがあったと判断し、その旨を記した識別結果情報を作成する。不正な改ざんがない場合、カメラ識別情報Iを用いて、メモリ部16Bに記録されている機器登録情報を検索し照合する。照合結果、カメラが盗難された旨の盗難情報Aやデータ処理制御指示情報B等の照合結果情報が得られる。また、メモリ部16Bに記録されているカメラ登録情報を検索した結果、送信されてきたカメラ識別情報Iがカメラ登録情報内で検出されない場合、カメラ登録情報なしといった照合結果情報が得られる。作成された識別結果情報や照合結果情報は、通信回線によって、カメラ識別情報Iを送信したラボ店の入出力機14に送信される。

【0024】入出力機14では、送信されてきた識別結

果情報や照合結果情報に基づき、例えば、カメラ識別情報Iが改ざんされたと判断された識別結果情報の場合や、照合結果情報として盗難情報Aが得られた場合、入力機14Aでの画像処理や出力機14Bで行なうプリント画像の出力処理を停止し、撮影画像の出力を阻止する。

【0025】すなわち、所望の画像処理を施して処理画像データの出力の依頼を受けた撮影画像、あるいは、プリント画像の出力処理を受けた撮影画像が、盗難カメラで撮影された可能性が高いと判断され、画像処理を行わず、従って、処理画像の画像データを記録メディアに書き込まず、処理画像の提供を行なわない。また、プリント画像を出力せずプリント画像の提供サービスを行なわない。さらに、必要に応じて、盗難カメラで撮影された旨の情報を警察に通報するとよい。また、データ処理制御指示情報Bが得られた場合、制限されたデータ処理の内容に従って、データ処理が制限される。例えば、プリント出力画像の枚数やプリント出力画像のサイズに制限を加えたり、画像処理、またテンプレート画像との合成処理等に制限が懸けられる。また、カメラ登録情報なしといった照合結果情報が送信された場合、出力処理、画像処理、記録処理さらには合成処理等の各種処理が制限されず、要求されたサービスに従って処理を行なう。

【0026】このように、撮影画像データDの処理に制御を課することによって、例えば、親が正規に使用するカメラ12を子供に貸し与えた場合、貸しあてた日以前に親が撮影した画像をプリント出力して子供に見せたくない等の理由から、撮影画像のプリント出力処理を制限することができる。また、親が正規に使用するカメラ12を子供に貸し与えた場合、金銭感覚の希薄な子供が、高価な画像処理やテンプレート画像の合成処理を施したプリント画像を注文したり、必要枚数以上のプリント画像のプリント出力や必要以上に大きなプリント画像のプリント出力を注文しないように、撮影画像データDの処理内容を制御することができる。勿論、盗難されたカメラ12が第3者の手に渡り、このカメラ12で撮影された画像がプリントされないように、プリント出力処理を停止する制限を課することもでき、盗難されたカメラの利用価値は失われ、カメラの盗難は抑制される。

【0027】上記実施例は、カメラから出力された撮影画像データやフィルムに記録された撮影画像を出力情報とし、この出力情報から得られる画像データに対して施すプリント出力処理、画像処理、テンプレート画像との合成処理、モニタへの再生処理、あるいは、記録メディアへ書き込む記録処理等に制限を課するものであるが、本発明において出力情報は、音声機器による音声データであってもよく、また、携帯情報端末で作成した手書きデータや文書データであってもよく、また、撮像装置が設けられた携帯情報端末で撮像される静止画あるいは動画の画像データであってもよく、あるいは、携帯情報端末



で撮影された静止画あるいは動画の画像データ、および携帯情報端末の音声機器から得られた音声データ、および携帯情報端末で作成した手書きデータあるいは文書データのいずれか2つを組にした出力データであってもよい。この場合、処理として、各種データの出力処理や、画像処理や、各種出力データとの合成処理、モニターやスピーカ等への再生処理、あるいは、記録メディアへ書き込む記録処理等である。また、携帯電話やPHS等の通信機器の出力する付属情報を出力情報に加えてもよい。一般に携帯情報端末は、携帯電話やPHS等の通信機器に接続されて通信を可能とするため、携帯情報端末等から出力された出力情報を通信機器を用いて送信する送信処理を本発明における制御対象としてもよい。

【0028】次に、本発明の機器の動作制御方法について説明する。

【0029】図3には、本発明の機器の動作制御方法を実施するカメラの撮影制御システム30が示されている。カメラの撮影制御システム30は、カメラ32とパーソナルコンピュータ34とを有して構成される。

【0030】カメラ32は、パーソナルコンピュータ34と無線等によって通信を可能とする通信装置を備え、一定時間毎にあるいは、必要な時に、例えば画像を撮影する時に、通信装置を介して動作許諾信号をパーソナルコンピュータ34に送信するように構成される。パーソナルコンピュータ34は、カメラ32の正規の使用者が管理するコンピュータであって、カメラ32から動作許諾信号を受けると、直ちに暗号化された動作制御指示情報をカメラ32に送信する送信装置を備える。ここで、動作制御指示情報は、カメラ32の動作、例えば撮影許可あるいは撮影禁止の指示情報や、撮影枚数を制限する指示情報や撮影ズーム倍率を制限する指示情報や、デジタルスチルカメラの場合、撮影された画像データの記録メディアへの書き込み記録処理を許可するあるいは禁止する指示情報や、撮影画像の表示画面への表示の許可あるいは禁止の指示情報等、カメラ32の各動作を全面的に許可、部分的に許可あるいは全面的に禁止する各種動作の指示情報である。

【0031】カメラ32は、動作制御指示情報を受信する場合のみ、動作制御指示情報に従って、動作が許可される範囲内で撮影動作を行えるように構成される。なお、暗号化された動作制御指示情報は、カメラ32が備えるCPUで解読され、動作制御指示情報がカメラ32の作動する各部分に送られる。動作制御指示情報を暗号化することで、第3者が正規の使用者の代わりにカメラ32の動作を許可してカメラ32で撮影を可能とすることを防止することができる。カメラ32が盗難された場合、パーソナルコンピュータ34がカメラ32に送信する情報をカメラの動作を全面的に禁止する動作制御指示情報に変更し、盗難カメラが正規の使用者以外の第3者によってカメラ32が容易に動作しないように設定す

る。

【0032】このような通信機能を備えるカメラ32は、携帯電話の機能やPHS機能を付加することによって実現することができる。また、本実施例では、カメラ32が通信する通信先は、正規のカメラ使用者が管理するコンピュータであるが、本発明ではこれに限定されず、その他に、例えば、事前に契約して登録した最寄りのラボ店やコンビニエンスストア等が管理するコンピュータであってもよい。

【0033】さらに、カメラ32の通信相手先を、正規の使用者が常時身につけ所持する通信機能付IDカードやPDA（携帯情報端末）等に設定してもよい。通信機能付IDカードの場合、例えば、非接触型ICカードを用いたマイクロ波方式による通信方法を用い、あるいは、携帯情報端末の場合、近距離データ通信の無線インターフェース規格であるBluetoothにより通信するとよい。例えば、通信機能付きIDカードは、カメラ32の正規の使用者が服のポケットに入れて身につけ、あるいは所持する鞆等に入れて持ち運ぶため、正規の使用者がカメラ32を使用する場合、通信機能付きIDカードと通信し、暗号化された動作制御指示情報を通信機能付きIDカードから受信することができる。カメラ32が盗難されて正規の使用者から離れた場合、通信が不能となり、動作制御指示情報を得ることができない。このように通信が不能となり、動作制御指示情報を得ることができない場合、カメラ32の撮影動作を停止するようにカメラ32は構成される。また、カメラ32が盗難された場合、正規の使用者の通信機能付きIDカードやPDA（携帯情報端末）等がカメラ32に向けて発信する情報を全面的にカメラの動作を禁止する動作制御指示情報を設定する構成としてもよい。

【0034】このように、カメラが正規の使用者から離れ、予め定められた通信先とカメラ32の通信が不能となり、カメラ32の動作を自動的に停止し、カメラの撮影を不可とするので、カメラの盗難を抑制することができる。

【0035】上記例では、カメラの撮影動作を制御の対象としたが、本発明ではこれに限定されない。例えば、デジタルスチルカメラの場合、デジタルスチルカメラで撮影した撮影画像をPCカードやフラッシュカード等の記録メディアに記録する書込処理を制限する制御や、ケーブルを介して撮影画像データをコンピュータに転送する転送処理を制限する制御であってもよい。あるいは、コンピュータ等から画像データの転送を受ける転送処理を制限する制御であってもよい。

【0036】さらに、本発明においては、カメラにとどまらず、通信機器や電子機器であってもよく、このような機器に記録されている静止画や動画の画像データや音声データの再生処理、すなわち、画像を表示画面に再生し、あるいは、画像再生に音声同期させて出力させる

再生処理を制限する制御や、上記各種データや特定のソフトウェアで処理された処理データ等を外部機器に転送する転送処理を制限したり、また、手書き入力データや文書データの画像表示を制限する制御や外部機器に転送する転送処理を制限する制御であってもよい。さらに、機器に組み込まれている特定のソフトウェアの実行を制限する制御であってもよい。また、別の外部機器から転送される画像データや音声データの受け取りを制限したり再生処理を制限する制御や、外部機器から転送される手書き入力データや文書データ画像の受け取りを制限したり、画面表示を制限する制御であってもよく、さらに、外部機器から転送されたデータを用いてソフトウェア処理する特定のソフトウェアの実行を制限する制御であってもよい。このような制御は、全面的禁止あるいは全面的許可の他に、部分的許可あるいは部分的禁止を行なう制御も含まれる。

【0037】また、上記実施例では、パーソナルコンピュータ34から動作全面禁止、あるいは、警告メッセージの表示等の動作制御指示情報が得られた場合、また、通信機能付IDカードやPDA（携帯情報端末）等と通信不可能な場合、電源断においてもカメラ32の画像表示画面に警告メッセージ、例えば盗難警告メッセージを継続表示するように画像表示を制御するものであってもよい。図4に示すように、カメラ32の画像表示画面に盗難品である旨が表示されると、盗難カメラが第3者の手に渡ることは少なくなり、また第3者がカメラ32を用いて人前で使用しづらくなり、盗難カメラの使用が抑制される。このような盗難警告メッセージの表示は、パーソナルコンピュータ34がカメラ32に送信する情報を動作の禁止を解除する動作制御指示情報を設定することによって、あるいは、通信機能付IDカードやPDA（携帯情報端末）等と通信が可能となる場合等において解除することができる。

【0038】なお、電源断においてもカメラ32の表示画面に盗難警告メッセージを継続表示する方法は、カメラの電源断の際にも、液晶表示パネルの表示画面を常時ON状態とする構成のものであってもよいが、好ましくは、特開平11-316397号公報に記載される電子ディスプレイに適用する電気ペーパーシート（電子ペーパー）、あるいは、ASCI12000年2月号220頁～225頁および3月号242頁～247頁に掲載されている電子ペーパーを用いるのがよい。

【0039】電子ペーパーとは、上記公報および、上記掲載記事によると、2枚のプラスチックシートの隙間のオイル液内に自由に浮遊している白黒半分ずつに塗り分けられた極小の無数の球にプラスチックシートの外側から電界を加えることによって、球を回転させて固定することができ、その際、球の回転によって白黒の面をプラスチックシートの表に向かせて、白黒の図柄や文字を浮き上がらせることができ、この原理をカラーの画像に適

用することができるものである。この電子ペーパーは、液晶表示媒体と同様に表示媒体として今後大いに用いられることが予想される。また、電子ペーパーとして、多数の白い球を内部の青い液体中に浮遊させた直径10分の1mm程度の透明なマイクロカプセルを2次的に敷きつめたシートを両面から電界を加え、クローン力によってマイクロカプセル内の白いカプセルを一方方向に移動させることで、白い球が一方方向に移動したマイクロカプセルの部分のシートの色を青から白に変えることができ、この原理を用いてカラー画像を再現する電子ペーパーも提案されている。また、強誘電性液晶を用いたフィルム液晶も電子ペーパーとして提案されている。

【0040】このような電子ペーパーでは、電界を与えて一度表示された画像が次の電界が加えられるまで消えず保持される利点や、また、次の電界が加えられるまで画像が保持されるため、従来の液晶ディスプレイに比べて電力消費が少なく済むといった利点や、液晶ディスプレイのように見る方向によって画像の濃淡が極端に変化する視野角依存性も持たないといった利点を有する。このような電子ペーパーをカメラ32の表示画面に用いることで、カメラ電源ONの際は勿論、カメラ電源断の際にも盗難警告メッセージを継続表示し、他人に視認し易いように表示することができる。

【0041】以上、本発明の出力情報の処理制御方法および機器の動作制御方法について詳細に説明したが、本発明は上記実施例に限定はされず、本発明の要旨を逸脱しない範囲において、各種の改良および変更を行ってもよいのはもちろんである。

【0042】

【発明の効果】以上、詳細に説明したように、パスワード等の入力の手間をかけず、情報通信機器や電子等機器等から出力された出力情報に施す処理を制御し、あるいは、情報通信機器や電子等機器等の動作を制御することができ、第3者の使用を制限することができる。さらには機器の盗難を抑制することもできる。

【図面の簡単な説明】

【図1】 本発明の出力情報の処理制御方法の一例を実施する出力データの処理制御システムを示す説明図である。

【図2】 本発明の出力情報の処理制御方法で用いる機器登録情報の一例を示す図である。

【図3】 本発明の機器の動作制御方法の一例を実施するカメラの撮影制御システムを示す説明図である。

【図4】 本発明の機器の動作制御方法の他の例を示す説明図である。

【符号の説明】

10 出力データの処理制御システム

12、32 カメラ

14 入出力機

14A 入力機

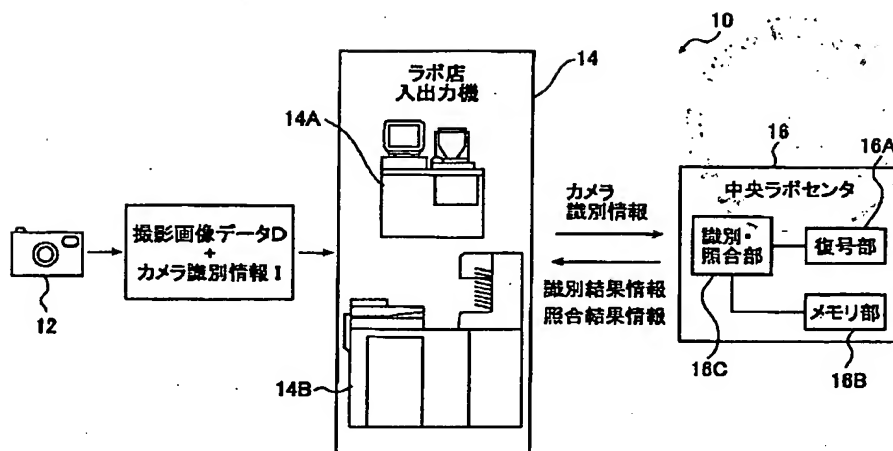


14B 出力機  
16 コンピュータ  
16A 復号部  
16B メモリ部

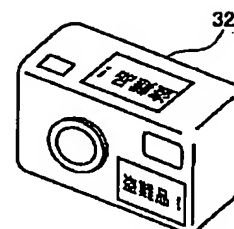
\*16C 識別・照合部  
30 カメラの撮影制御システム  
34 パーソナルコンピュータ

\*

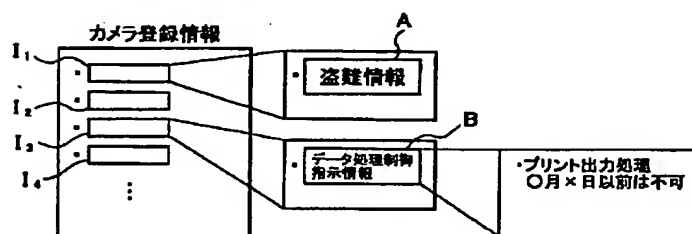
【図1】



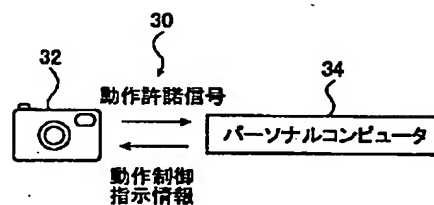
【図4】



【図2】



【図3】



フロントページの続き

(51)Int.Cl.

H04N 7/081

// H04N 101:00

識別記号

F I

H04N 7/08

テーマコード (参考)

Z